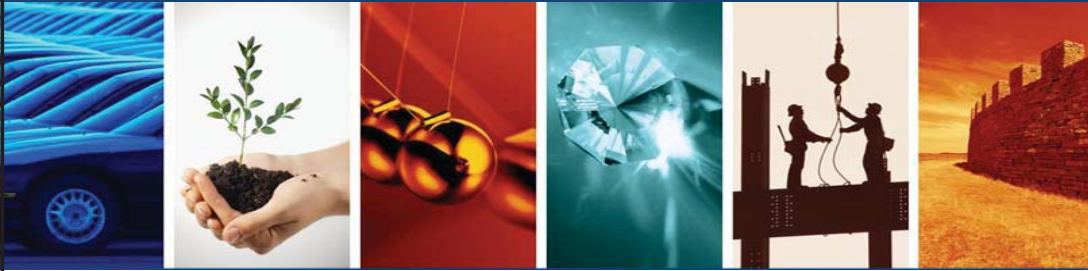


資訊時代的資訊安全 挑戰與機會

Prepare for the worst, don't hope for the best

Peter Pu (蒲樹盛), Vice President (副總經理), BSI 英國標準協會
peter.pu@bsigroup.com



raising standards worldwide™



Content 內容



- Risk Awareness
資訊時代之風險意識
- Information Security & Risk Management
資訊安全與風險管理
- Information Security & Regulation
資訊安全與法令

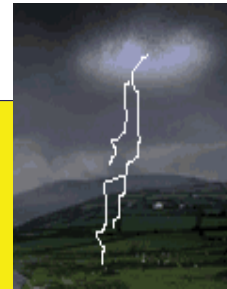
raising standards worldwide™



營運與危機 - 如何預料無法預料的事 (Expect the unexpected)

- 組織容易發生何種危機？何時發生？如何發生？如何預防？如何處理此種危機？
- 企業管理必備之管理技能

經濟蕭條 天災事件 恐怖活動
資訊外洩 戰爭 人為疏失 火災
掏空資產 員工舞弊 傳染病
惡意競爭 人力短缺
財務問題 重大失事 系統中斷



raising standards worldwide™



The future of Management 管理未來

新的管理思維正在淘汰舊的商業模式



raising standards worldwide™



權威財經雜誌「富比世」報導美國勞工部的預測

【聯合報／編譯組／綜合報導】



至2014年之預測:

- 前景佳之行業: 醫療照顧、教育和金融服務業。
- 前景差之行業: 製造業(-5%)、紡織業操作員(-36%)、電腦程式設計師(+2%)、新聞記者(+5%)、廣播電台(-5%)、政府僱員等(需求銳減或是漲幅有限, 檔案管理員工作-36%)。
- 有志者最好朝更專業的方向發展, 例如 資通安全。
- 豪華和特殊旅行及旅遊支出增加。
- 不要過份擔心自己希望從事的職業成長預期不佳。即使該行業正在萎縮, 只要能發揮所長, 就能在那一行中脫穎而出。

raising standards worldwide™



資訊時代 安全風險增加

資安事件頻傳

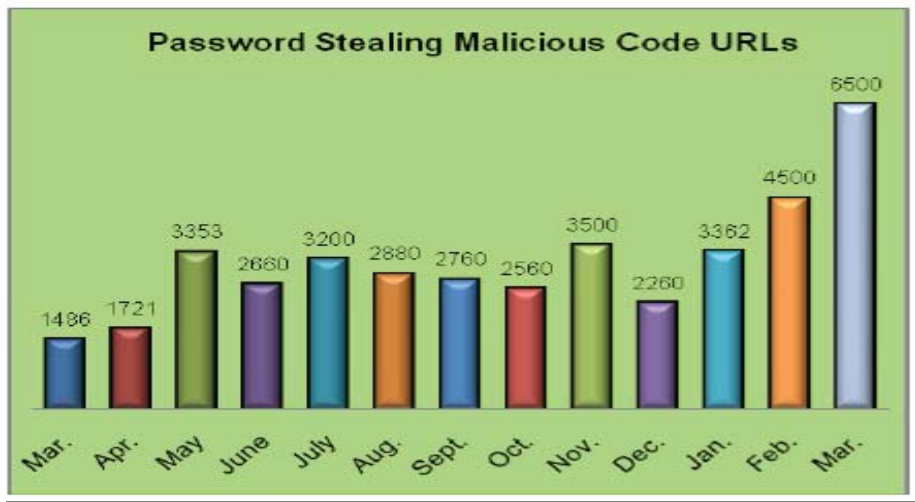


raising standards worldwide™



Phishing Activities Trends Report

Q1 2008- APWG (Anti-Phishing Working Group)



raising standards worldwide™



釣魚網站竊個資 台灣猖獗

- 「釣魚網站」已是國內外嚴重的詐欺犯罪型式；
- 台灣是亞太暨日本地區網路惡意活動排名第三的國家。
- 國際知名網路資訊安全業者賽門鐵克報告指出，在亞太暨日本地區，台北是擁有最多釣魚網站的城市，而台灣是感染傀儡程式第二多的國家；由人口密度看，台灣是亞太暨日本區網路惡意活動排名第三的國家。

raising standards worldwide™



2008 Internet Security Threat Report

Current Rank	Previous Rank	Country/Region	Current Percentage	Previous Percentage	Bot Rank	Command-and-Control Server Rank	Phishing Web Sites Host Rank	Malicious Code Rank	Spam Zombies Rank	Attack Origin Rank
1	1	China	38%	42%	1	2	1	1	1	1
2	2	South Korea	14%	14%	3	1	2	5	2	2
3	4	Taiwan	12%	12%	2	3	5	2	4	3
4	3	Japan	8%	13%	4	4	4	3	6	4
5	5	India	6%	7%	11	11	13	2	9	16
6	6	Australia	5%	5%	5	5	3	4	10	5
7	7	Thailand	4%	4%	9	6	6	11	3	9
8	8	Malaysia	4%	2%	6	7	7	7	7	7
9	9	Singapore	2%	2%	7	8	10	6	9	6
10	10	Philippines	2%	1%	8	10	14	8	8	8

Table 1. Malicious activity by country, APJ
Source: Symantec Corporation

raising standards worldwide™



Malicious Codes

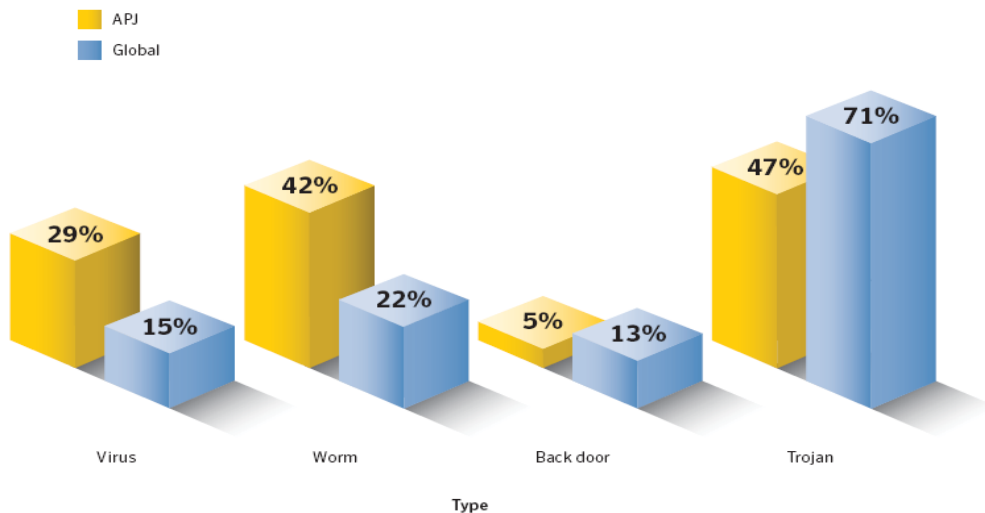


Figure 2. Malicious code types, APJ and Global
Source: Symantec Corporation

raising standards worldwide™



Malicious Codes

Rank	Sample	Type	Top Reporting Country/Region	Second Reporting Country/Region	Vectors	Impact
1	Gampass	Trojan	China	Taiwan	N/A	Steals online gaming passwords
2	Fujacks	Worm/virus	India	China	CIFS	Modifies HTML files
3	Mumawow	Virus	China	Taiwan	CIFS	Downloads other threats
4	Gammima	Worm	Taiwan	Australia	CIFS	Steals online gaming passwords
5	Looked	Worm/virus	Taiwan	China	CIFS	Disables security applications
6	Rontokbro	Worm	India	China	SMTP	Performs DoS attacks
7	Netsky	Worm	Japan	Singapore	SMTP	Logs keystrokes
8	Fubalca	Worm/virus	China	Japan	CIFS	Downloads other threats and modifies HTML files
9	Looked.P	Worm/virus	Taiwan	China	CIFS	Disables security applications
10	Adclicker	Trojan	China	Australia	N/A	Clicks advertisements to generate revenue

Table 10. Top 10 regional malicious code samples, APJ

Source: Symantec Corporation

raising standards worldwide™



可攜式裝置「毒來毒往」

- 越來越多人使用隨身碟存取資料，危害最大的惡意程式都是透過感染USB裝置來散布，這類可攜式裝置已成為資訊安全漏洞。
- 線上購物網站易被駭 須防個資外洩
- 2008年-會員人數眾多的社交網站、熱門購物網站、線上遊戲網站、部落格，會持續成為駭客攻擊對象，透過電子郵件寄發木馬程式或釣魚網站，收集網友的帳號密碼。
- 可攜式裝置如智慧型手機、MP3隨身聽、隨身碟等，近年成為駭客利用突破安全防線媒介，而公共區域的無線基地台，則將成為惡意攻擊的散播點。

raising standards worldwide™



Foxy分享軟體 機密遭竊取

人員違反資安規定，利用隨身碟將資料帶回家作業，導致資料被家中電腦裡的木馬病毒竊取外洩。



raising standards worldwide™



世界標準日 (World Standards Day)

- 每年慶祝國際建立共識的日子
- 每個組織都想要改善自己的營運方式，提升競爭力、降低成本、更有效地管理風險，及改善顧客滿意度。



raising standards worldwide™



Management Systems


Information Security

- Security Policy
- Systems Development
- Information Backup
- Access Controls
- Network technology

BCM
(Business Continuity Management)

Organization Management

raising standards worldwide™




Operational Risk 作業風險

risk that deficiencies in information systems or internal controls will result in unexpected loss


資訊系統或內部控制不足，將導致意外損失的風險。

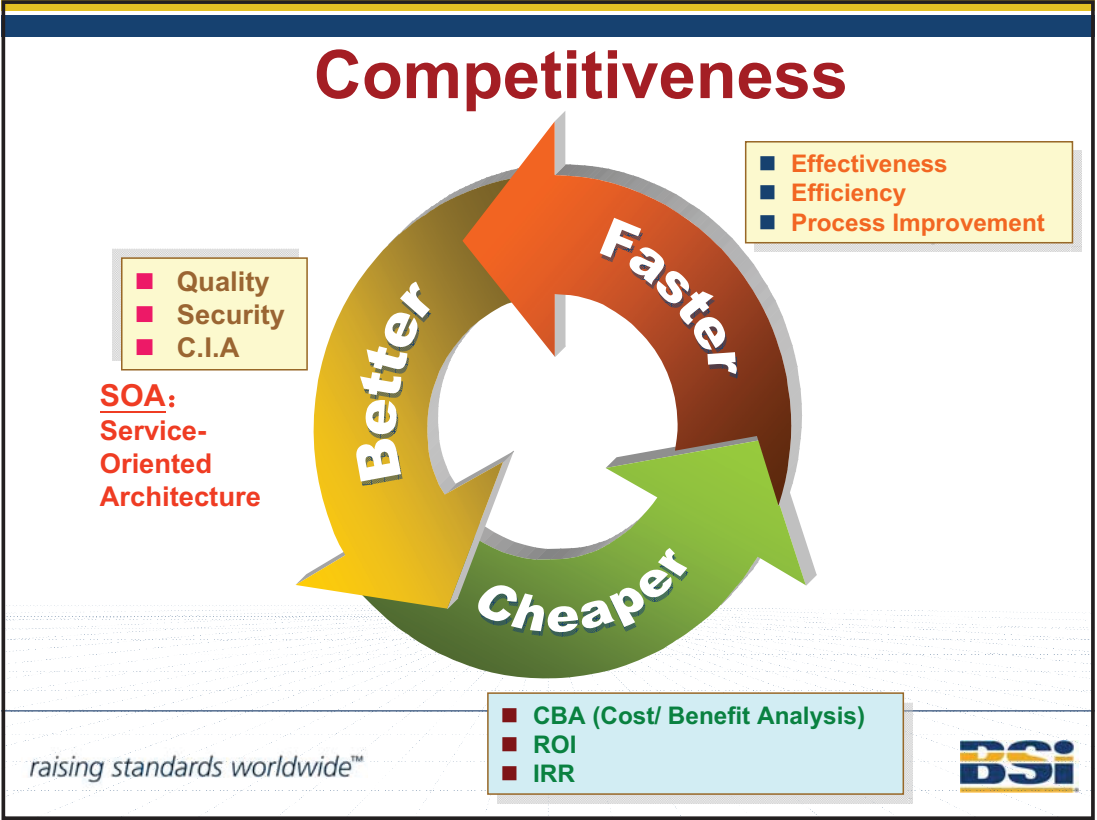
NOTE :This risk is associated with human error, system failures and inadequate procedures and controls.

注意：此風險與人為錯誤、系統失效以及不當程序及控制有關。



raising standards worldwide™





Better- 台灣首部「資通安全政策白皮書」

工商時報 2008.03.15

台灣資通安全產值將於二〇〇九年達到五七二億元的歷史新高(行政院科技顧問小組引用市調機構調查)

但我國對資安防護的投資比重仍落後韓國、新加坡及日本等國，顯示台灣在資安防制警覺性並不如日、韓各國。

■資安關鍵指標(呈現我國資安發展現況):

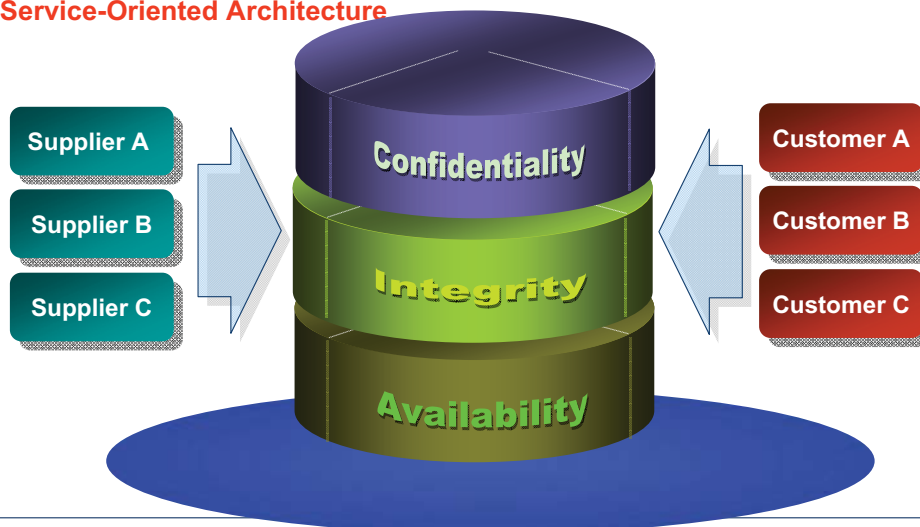
- 國內市場，目前防毒產品使用率已達90.7%，
- 防火牆使用率達67.5%。
- 各機關(構)通過國際資訊安全管理系統驗證數，迄三月止，已達170家，全球排名第四。
- 入侵偵測系統21.9%、
- 漏洞修補程式管理20.2% (建置率不足)，
- 組織遭受資安事件侵害比例高達51.8%。

raising standards worldwide™



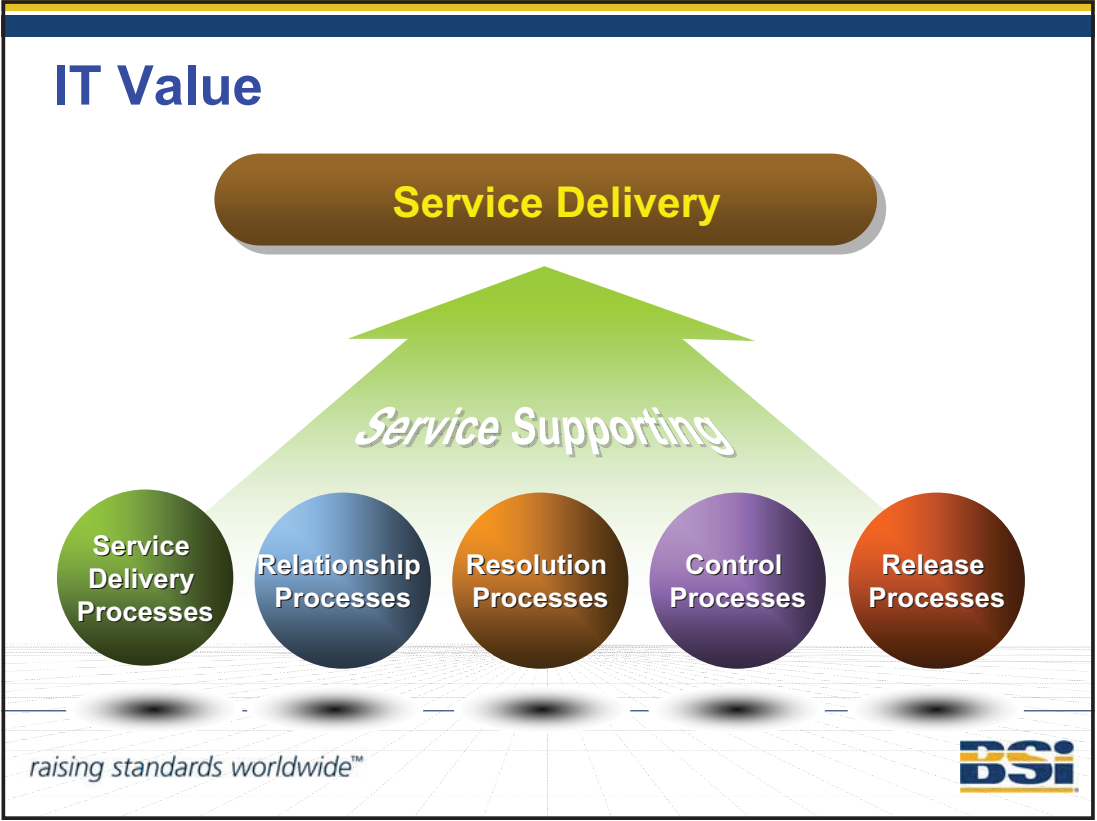
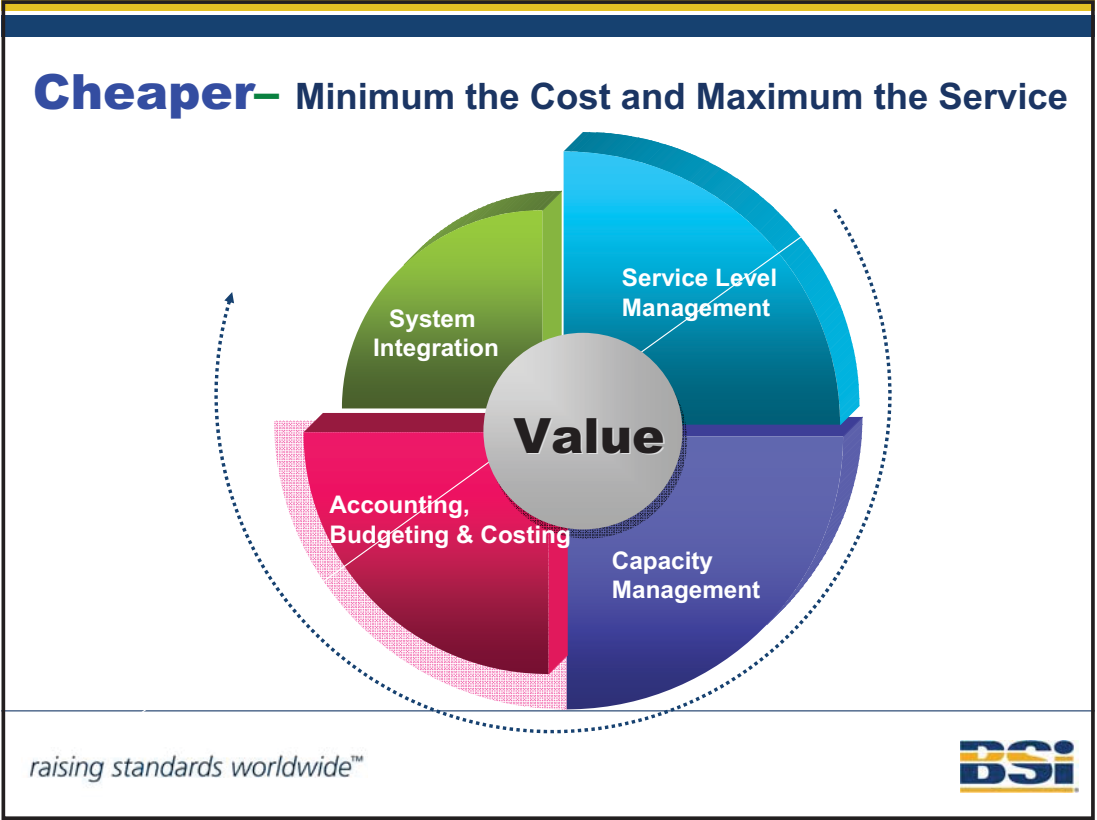
Better – Quality & Information Security

SOA:
Service-Oriented Architecture



raising standards worldwide™





Compliance

raising standards worldwide™

BSI

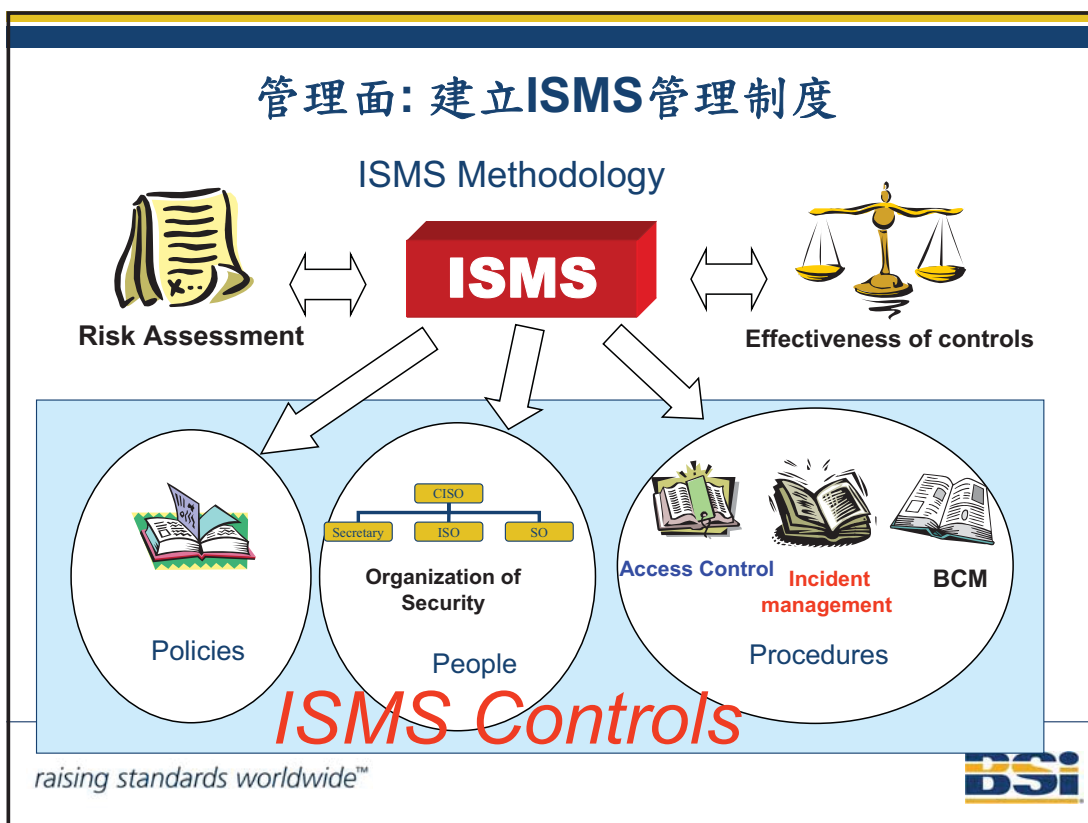
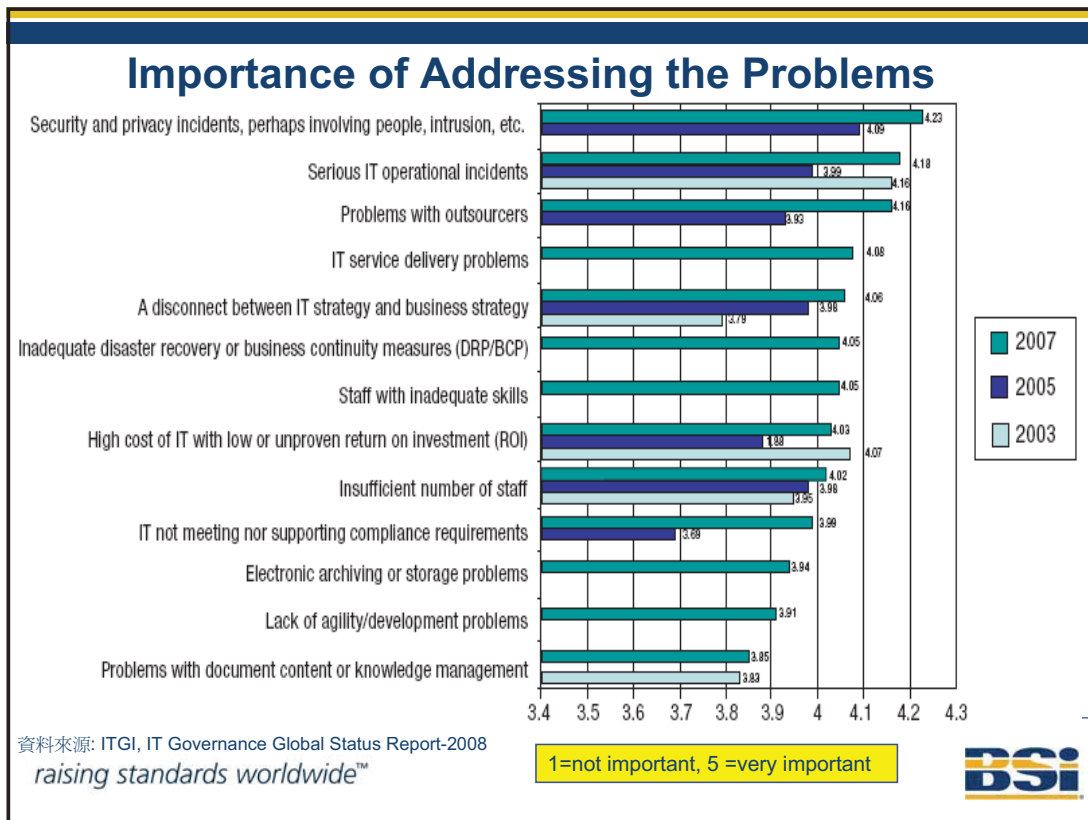
Strategy

- A **Strategy** is a long term plan of action designed to achieve a particular goal.
- Strategy is differentiated from tactics or immediate actions with resources at hand by its nature of being extensively premeditated, and often practically rehearsed.
- Strategies are used to make the problem easier to understand and solve.
- The word derives from the Greek word *stratēgos*, which derives from two words: **stratos (army)** and **ago (ancient Greek for leading)**. *Stratēgos* referred to a "military commander" during the age of Athenian Democracy.
- **Strategy** is about choice, which affects outcomes.

From Wikipedia

raising standards worldwide™

BSI



認識法律

刑法妨害電腦使用專章

■ 第36章規範四種犯罪行為

- 無故入侵電腦罪 (第358條)
- 保護電磁紀錄規定 (第359條)
- 干擾電腦系統及相關設備罪 (第360條)
- 製作專攻電腦犯罪之程式罪 (第362條)

raising standards worldwide™



無故入侵電腦罪(第358條)

- 無故輸入他人帳號密碼、破解使用電腦之保護措施或利用電腦系統之漏洞，而入侵他人之電腦或其相關設備者
- 處3年以下有期徒刑、拘役或科或併科10萬元以下罰金
- 告訴乃論
- 對於公務機關之電腦或其相關設備犯罪者，加重其刑至1/2

raising standards worldwide™



保護電磁紀錄規定(第359條)

- 無故**取得**、**刪除**或**變更**他人電腦或其相關設備之電磁紀錄，致生損害於公眾或他人者
- 處5年以下有期徒刑、拘役或科或併科20萬元以下罰金
- 告訴乃論
- 對於公務機關之電腦或其相關設備犯罪者，加重其刑至1/2

raising standards worldwide™



干擾電腦系統及相關設備罪(第360條)

- 無故以**電腦程式**或其他**電磁方式**干擾他人電腦或其相關設備，致生損害於公眾或他人者
- 處3年以下有期徒刑、拘役或科或併科10萬元以下罰金
- 告訴乃論
- 對於公務機關之電腦或其相關設備犯罪者，加重其刑至1/2

raising standards worldwide™



製作專攻電腦犯罪之程式罪(第362條)

- 製作專供犯本章之罪之電腦程式，而供自己或他人犯本章之罪，致生損害於公眾或他人者
- 處5年以下有期徒刑、拘役或科或併科20萬元以下罰金

raising standards worldwide™



其他法律

- 電腦處理個人資料保護法
- 智慧財產權
- 組織營業秘密法
- 政府資訊公開法
- 電子簽章法

raising standards worldwide™



員工電腦灌盜版軟體 一經查獲公司負責

(2008/06/18)

- 推行反盜版的台灣商業軟體聯盟表示，外勤業務人員用的筆記型電腦，無論是公司配發或私人的電腦，只要是公務使用，公司就必須負責灌正版軟體，不然一經查獲，依照我國著作權法的保護，公司負責人必須負擔相關的法律責任(負擔高額的民事賠償，甚至刑事責任)。
- 隨著國人對著作權的重視，國內商用軟體盜版率逐年下降，從2001年盜版率一半以上(53%)，到去年為止已經降到40%。
- 台灣商業軟體聯盟曾經查過上市、櫃公司正版軟體使用情況，曾經有一間公司因此被判必須負擔2000萬元的罰款。
- 著作權法有分民事和刑事兩部分刑責，民事部分依照侵權金額計算賠償，而刑事部分最高可處五年以下有期徒刑。

raising standards worldwide™



組織安全與員工責任

- **改變心態觀念正確:**將是資安成功關鍵,要讓安全成為每一位員工的最優先考量的;若認為安全僅是資訊技術人員的責任,其結果是造成安全常常出現漏洞。強調每一位員工對整體安全所能帶來的貢獻。
- **安全訓練有效預防:**管理應該在安全訓練上投資，並且教育員工瞭解最佳的行事方式及技術知識。
- **安全政策之制定與落實:**清楚訂定完整的安全規範。建立負責任的文化，將安全預警視為是日常工作的一部份。
- **善盡責任強調風險:**每一個人都必須為自己所被指派的領域負起個人責任。：
 - 不開啟不明來源的電子郵件夾檔、
 - 遵守日常工作的安全守則
 - 不將敏感或機密文件隨手亂放
 - 通知適當的專業人員來解決IT問題，而不是自己私下處理。

Contribution 貢獻

raising standards worldwide™

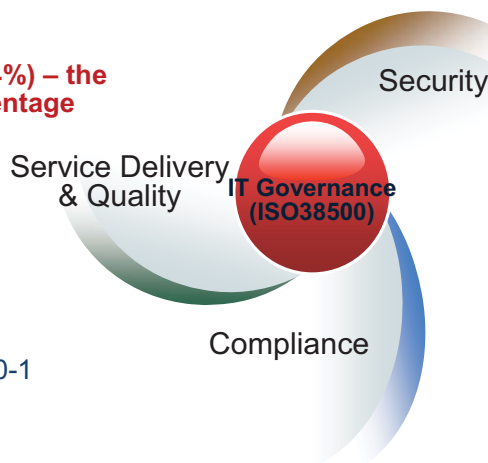


IT Governances Standard/ Best Practice

組織可用來強化其IT治理之標準或最佳實務

▪ Standards

- **ISO 20000 (24%) – the highest percentage**
- ISO 9000
- ISO 27000
- BS 25999
- ISO TR13335
- ISO/IEC12207
- ISO/IEC 19770-1



▪ Best practices

- **ITIL**
- COBIT
- CMMI
- IT Balanced Scorecard (BSC)
- Six Sigma
- PRINCE 2
- Other
 - ASL Application Services Library
 - MOF
 - Sourcing

raising standards worldwide™



***If your organization is not safe,
your future is not secure!***



Thanks